A METHOD OF SALE AUDITING IN PRIVATE TRANSACTION OF E-GOODS

FIELD OF INVENTION

The present invention relates to online digital commerce, and in particular online secure and private retail of digital goods.

BACKGROUND OF INVENTION

In the situation where an online merchant is selling goods it is desirable to keep the information about which digital goods the customers wishes to buy away from the merchant. One attempt to achieve such privacy protection is described by F. Bao, R. Deng and P. Feng, in "An efficient and practical scheme for privacy protection in the e-commerce of digital goods", Proc. of ICISC'2000 (International Conference on Information Security and Cryptography), LNCS, Springer-Verlag, 2001, which exploits an anonymizer service and some cryptographic techniques. Bao claims to provide a system, whereby a customer is able to buy a digital object from an online merchant without the merchant knowing which object is actually sold to the customer.

In the scheme of Bao, the merchant encrypts all his/her digital objects and puts them on a free-download server so that any customer can freely and anonymously download any of them. To actually obtain the downloaded digital objects, the customer must pay for the decryption of the digital object. By some cryptographic techniques, the customer can ask for "blinding decryption" so that the merchant cannot get to know what is the decrypted object.

However, except for the scheme of Bao the majority of prior attempts are too complicated in complexity to be implemented in reality, and are largely just theoretical solutions. That is, they are not commercially practical as they largely use bit-by-bit processing.

Further whilst it is desirable to enable a customer to purchase products secretly, sometimes it is necessary for the merchant to obtain statistic numbers about how many copies of digital objects are sold for business reasons. If the scheme in Bao is used for customers' privacy protection, the merchant cannot obtain accurate statistic numbers.

The statistic numbers on how many times each encrypted object is downloaded from the free-download server could reflect in certain degrees which digital object has been downloaded and how many times. But the numbers can not precisely reflect the number of each object being sold since it is possible for a customer to download without finally paying for the decryption. Those numbers can be used for presumedly sale auditing on how well each digital object sells. But for royalty purpose, those numbers are inaccurate.

It has not previously been thought possible to provide for trade in online goods, such that a merchant is unaware of what product a consumer has purchased, but is able to obtain statistics regarding products sold.

OBJECT OF THE INVENTION

It is therefore an object of this invention to develop a practical system that enables a customer to purchase digital products online from a merchant in private, such that the merchant is unaware of what product the customer has purchased.

A further object of the present invention is to provide a system whereby the merchant is able to obtain accurate details of which products have been purchased without compromising the secrecy of the customer.

SUMMARY OF THE INVENTION

With the above objects in mind the present invention provides in one aspect a method for trading digital goods online between a merchant and customer including the steps of:

the merchant encrypts each digital good with respective unique keys to create encrypted goods;

the merchant encrypts each respective unique key with a common key to create respective encrypted keys;

the merchant making the encrypted goods and the respective encrypted keys available to the customer;

the customer downloading one encrypted good and respective encrypted key;

the customer adding a customer encryption to the respective encrypted key to create a combined key, and returning the combined key to the merchant;

the merchant removes common encryption from the combined key using the common key to create a customer encrypted key, and returns the customer encrypted key to the customer;

the customer decrypts the customer encrypted key to obtain the respective unique key and uses the respective unique key to decrypt the digital good.

In the preferred arrangement the merchant would only remove the common encryption following payment from the customer for the goods in question.

As the customer has added a customer encryption to the encrypted key, the merchant is unaware of what key is being processed even when the common encryption is removed.

The digital goods could include one or more digital products, for example a set of books or a book and music combination.

In the preferred arrangement each digital product will be individually encrypted, although in some circumstances it may be desirable to group products together. This individual encryption ensures a customer only receives a single good for each purchase.

In a further aspect the present invention provides a method for trading digital goods online between a merchant and customer including the steps of:

the merchant encrypts each digital good with respective unique keys to create encrypted goods;

the merchant obtains parameters from an auditing centre;

the merchant encrypts each respective unique key with a common key and uses the parameters to create respective encrypted keys;

the merchant makes the encrypted goods and the respective encrypted keys available to the customer;

the customer downloads one encrypted good and respective encrypted key;

the customer adds a customer encryption to the respective encrypted key to create a combined key, and returns the combined key to the merchant;

the merchant removes common encryption from the combined key using the common key to create a customer encrypted key, and returns the customer encrypted key to the customer;

the customer decrypts the customer encrypted key to obtain the respective unique key and uses the respective unique key to decrypt the digital good.

If the merchant wishes to obtain sales statistics then the merchant collects transcripts from when the common encryption is removed, and forwards the transcripts to the auditing centre;

the auditing centre reviews the transcripts and obtains the parameters;

the parameters being able to identify what goods were sold.

In yet a further aspect the present invention provides a system for trading digital goods online between a merchant and customer wherein said goods are encrypted using parameters provided by an auditor, said customer obtaining said encrypted goods using blinding decryption such that said merchant is unable to identify said digital goods, said merchant providing

transcripts of sale transfers to said auditor, said auditor using said transcripts and said parameters to identify goods transferred.

BREIF DESCRIPTION OF THE DRAWINGS

Figures 1 and 2 provide a diagrammatic analogy of how the present invention works.

Figure 3 provides an overview flowchart of the preferred embodiment.

DETAILED DESCRIPTION

The present invention provides a system to allow an online merchant to sell products without knowing which products a customer actually buys and further allows the merchant to discover how many and what products have been sold, through the help of a trusted party auditing centre without compromising the privacy of the customer. The system is applicable for any digital products, including books, video, music, article, map, magazine, etc, in digital form.

The preferred embodiment actually includes two aspects, firstly how to blind the merchant such that the merchant does not know what is sold to the customer, and secondly, how to let the merchant discover the sale statistics data.

To better understand the system we refer to Figures 1 and 2 which provides an analogous example.

If we firstly consider the first aspect, namely how to blind the merchant such that the merchant does not know what is sold to the customer, and refer to Figure 1.

Suppose the merchant has four books (not shown) for sale. The merchant puts the four books into four separate boxes (1, 2, 3, 4) and locks the boxes (1, 2, 3, 4) with different locks (9, 10, 11, 12). The merchant then

puts the four different keys (not shown) which can unlock the boxes (1, 2, 3, 4) into four further boxes (5, 6, 7, 8) but locks them with a common lock (13). The merchant then groups the boxes accordingly, that is box (1) having book A inside and box 5 having the key to unlock lock (9) inside are grouped together (14). Similarly box (2) having book B inside, and box (6) having the key to unlock lock (10) inside, are grouped together (15). These groups (14, 15, 16, 17) may then be put into a public place.

Suppose the customer wants to buy the 2nd book B. The customer downloads the second group (15). The customer then locks the box (6) that contains the key to unlock box (2) with the customers own lock (18). The customer then pays the merchant and gives the box (6) to the merchant. The merchant can unlock the lock (13) but can't see what is inside the box (6) since it is still locked by the customers lock (18). The customer can then unlock their own lock (18) and get the key to unlock box (2), then unlock the merchants lock (10) to get the 2nd book B.

Rather than the customer paying for each individual transaction the system could also be used with a membership model. That is, a customer pays a certain amount of money that allows for a fixed number of digital goods to be obtained within a set time period.

Continuing the analogy and considering the second aspect, namely how to let the merchant discover the sale statistics data and referring to Figure 2. The same procedure as shown in Figure 1 is used, however this time the boxes (5, 6, 7, 8) that contain keys are from a sale auditing centre. The sale auditing centre paints numbers (19, 20, 21, 22) on the boxes (5, 6, 7,8) with a sort of special ink, which can only be seen by the auditing centre. No other person can see the numbers (19, 20, 21, 22). The merchant periodically collects all the transacted boxes and sends them to the sale auditing centre for statistics data. The sale auditing entire is then able to provide statistics as to which boxes where purchased by customers and hence which products were sold.

The above description is just an analogy for easy understanding of the preferred method. In actuality there are no boxes.

It must be remembered that the present invention deals with digital objects. As such there is no need for physical boxes. Rather each object for sale is uniquely encrypted by the merchant. Each key to unlock the respective digital object is also encrypted using a common key. If a customer wishes to purchase a digital object, they download both the encrypted object and also the encrypted key. The customer then adds their own encryption to the encrypted key, and forwards this together with payment to the merchant. The merchant will then decrypt their portion of the key, and return the key with the customer's encryption back to the customer. The customer is then able to decrypt the key which in turn enables the customer to retrieve the digital object.

In considering the description a Customer may be considered as any party who buys digital objects online. A merchant may be considered as any party who sells digital objects online. A digital object provider may be considered as any party who provides digital objects to the merchants, and an auditing centre may be considered as a trusted party who conducts sale auditing.

Each merchant may sell digital goods from several providers and each provider may have several digital objects.

The preferred system does have a number of Security Requirements which include:

1) A customer is able to buy a digital object from a merchant without disclosing to the merchant what the object is; furthermore, the merchant ideally cannot even tell which provider the sold digital object originated from.

2) The customer can obtain only one digital object in one transaction. This is the protection to the merchant to prevent any customer obtaining two objects by paying for only one.

3) Later when necessary, the merchant can give the auditing centre all the transaction transcripts, from which the auditing centre can recover how many digital objects from each provider were sold.

4) Even with the transaction transcripts, the auditing centre cannot obtain any one of the digital objects.

The transaction transcript here refers to the ciphertext for blinding decryption, which is given to the merchant by the customer., as it is the ciphertext of the key that is used to encrypt the digital goods, instead of the ciphertext of the digital goods.

The model given above is general. We can also consider the situation where the merchant wants to know how many copies of each digital object are sold. That may be considered as a special case of the above situation where each provider has only one digital object.

Referring now to Figure 3, and considering the previous analogy. The main steps of the preferred system are shown namely:

a) The merchant (23) obtains (35) system parameters from the auditing centre (24). These parameters may be considered like the boxes with invisible numbers on them, such that only the auditing centre can see the number and will be defined shortly.

b) The merchant (23) obtains (26) the digital goods from the providers (25).

c) The merchant (23) encrypts (27) the digital goods with a conventional cryptosystem and encrypts the keys with the parameters from

the auditing centre. Then the merchant puts the encrypted digital goods on the free-download server (28) and the key for content keys on transaction server (29).

d) The customer (30) downloads (31) the encrypted digital goods freely and anonymously.

e) The customer (30) pays (32) for the keys that are used to encrypt the digital objects. The merchant (23) removes their encryption (32) enabling the customer (30) to decrypt the required digital object.

f) The merchant (23) puts the transcripts of the blinding decryption in step (e) into the transcript database (33).

g) The merchant (23) sends (34) the transcripts to the auditing centre (24) for provider-based sale statistics recovery.

It will be understood that if a merchant does not require sales statistics, then a sale auditing centre is not required and steps (f) and (g) are not necessary. Similarly steps (f) and (g) may be combined, such that transcripts are forwarded directly to the sale auditing centre and the transcripts database is omitted.

Now considering the steps in more detail.

Denotations

Assuming there are totally n providers, and that a merchant has m digital goods M_1, M_2, ...M_m. We Denote the fact that M_i is from the j-th provider by $M_i \in Provider_j$.

System Parameters

The auditing centre picks primes p, q_1, q_2,...q_t

such that $2^t > n$

and

$$p = 2\prod_{i=1}^{t} q_i + 1$$

where "*t*" is a parameter of the system, which determines how many content providers the system can support. It will be understood that there is a tradeoff between the number of providers that can be supported and the efficiency of the system.

Let q_p be a generator of $\mathbf{Z}_p^*$ and let

$$g = (g_p)^2 \bmod p \quad \text{and} \quad Q = \prod_{i=1}^{t} q_i .$$

Apparently *g* has order *Q*.

The auditing centre keeps $q_1, q_2, \ldots, q_t$ secret and publishes *p*, *Q* and $g_1, g_2, \ldots, g_n$ as the systems parameters, where

$g_i = g^{e_i} \bmod p$, $e_i = \prod_{j=1}^{t} (q_j)^{b_{ij}}$, b_{ij} is the *j*-th bit of *i* in binary format.

It is these system parameter g_1 which enable the sale auditing centre to provide sales statistics to the merchant, and following on from the earlier analogy may be considered the boxes within which the unique keys are locked.

For the merchant to encrypt the *m* digital goods and the keys the following steps can be taken:

1. Randomly choose *m* numbers $s_1, s_2, \ldots, s_m$.
2. Compute $r_1, r_2, \ldots, r_m$: if $M_i \in Provider_j$, $r_i = (g_j)^{s_i} \bmod p$.
3. Generate the keys by hashing r_i, K_i=MD5(r_i) for i=1,2,...,*m*.
4. Encrypt M_i by key K_i, C_i=AES(M_i, K_i) for i=1,2,...,*m*.
5. Randomly pick a secret number *d* and computes $e = 1/d \bmod Q$
6. Encrypt r_i with *e*, $D_i = (r_i)^e \bmod p$.

For the encryption r_j is generated from g_j, where g_j is received from the auditing center. From mathematics r_j has the same order as g_j. Similarly, D_j has the same order. The order is not known by the merchant. Only the auditing center knows the order. The center links the order with j, and keeps a list of such links. When the auditing center gives the g_j to the merchant (or just publishes all g_j's), the center tells what j is, but keeps the order secret. The merchant will use r_j to encrypt the digital goods from provider_j. Here from the previous analogy, Cj refers to the locked box containing digital goods from provider_j, and Dj refers to the locked box containing the key r_j.

In the following step 8, U is the encryption of Dj. Please note that U has the same order as Dj. But now the merchant does not know what j is associated with U since the merchant does not know what Dj is encrypted. The auditing center can discover j since the center is the only party who can compute the order of U and has the list to link orders with j.

For decryption of the digital goods the following steps may be followed:

The customer anonymously downloads $<B_i, C_i, D_i>$, and goes through the following blinding decryption.

7. The customer randomly picks a secret R and computes $S=1/R \bmod Q$.
8. The customer gives $U=(D_j)^S \bmod p$ to the merchant.
9. The merchant computes $V=U^d \bmod p$ and returns V to the customer.
10. The customer computes $K_j=\text{MD5}(V^R \bmod p)$ and $M_j=\text{AES}^{-1}(C_j, K_j)$.

where B_i can be, a short description of the digital goods, such as an abstract which assists the customer in deciding whether to purchase the goods or not, and is likely to be downloaded for free.

If we compare this to the previous analogy then R is like the padlock and S is like the key for R. Step 8 refers to locking D into a box, where U is the ciphertext of D. d is the merchant's key, and Step 9 refers to removing the merchant's lock from box U.

$V^R \bmod p$ is like opening the box by key R. MD5 is a hash function which hashes a long message to a short one (128 bits). This step is also done when the merchant encrypts the digital goods. This step is included as the length of D, U, V are all 1024-bit for security reasons, but the length of the key for AES (Advanced Encryption Standard) is 128-bit. So the actual key to encrypt digital goods is K. M_j=AES^{-1}(C_j, K_j) is the decryption of C with key K.

The steps 7, 8, 9 and 10 constitute blinding decryption of r_i. Since p is constructed in a special way, any party who knows q_1, q_2, ... , q_t can detect the order of any element of $\mathbf{Z}_p^*$. On the other hand, no one can change the order of an element of <g> with non-negligible probability unless they know q_1, q_2, ... , q_t. Of course we assume q_1, q_2, ... , q_t are large enough

Sale Auditing

Whenever the merchant wants to obtain statistics on how many digital goods from each provider are sold, the merchant submits all the blinding decryption transcripts, i.e., all the U's received at step 8 of all the transactions, to the auditing centre without telling the centre which U is from whom. The centre, who knows q_1, q_2, ... , q_t, can efficiently decide each U's order by checking

$U^{Q/q_j} \overset{?}{=} 1 \bmod p$ for j=1,2,...,t.

(If $U^{Q/q_j} = 1 \bmod p$, U's order has factor q_j)

If a U has the same order as g_i, it means that this U is for a sale of a digital object from the i-th provider.

The sale auditing is realized on the assumption that the merchant honestly conducts the step 2 of the scheme.

Performance Analysis

Computation Cost of Auditing Centre Generating the required p, q_1, q_2, ... , q_t is not infeasible. It can be done by first picking more than t primes, say $2t$ primes, then picking t of them and conducting prime test to 2 times of their product plus 1. The procedure can be repeated until a prime is obtained. The process is efficient due to the density of primes.

Ideally the size of each q_i should be 256-bit for security reasons, which will be explained later. The number t, therefore, determines both the size of p and the number of providers the system can support. For example, when t is 16, the system can support 65536 providers while p has 4097 bits. When t is 24, the system can support about 16 million providers while p has 6145 bits. In testing for the speed of the exponential computation modulo on such large numbers on a Pentium III 933MHz CPU with 256M memory using RedHat 7.0 operating system the results are acceptable. The average time for conducting an exponential computation modulo 4097-bit number with full-size exponent is about 0.3 second. The time for 6145-bit number is about 1 second. The time is basically linear with the length of the exponent when the module size is fixed. Therefore smaller exponents lead to shorter time, and the total time to determine the order of an element should not be much longer than that of an exponent computation with full-size exponent.

Computation Cost of Merchant The most common computation the merchant conducts is the decryption operation $V=U^d \bmod p$. The encryption operation $D_i=(r_i)^e \bmod p$ is conducted only once for each digital products M_i. The decryption operation is as often as the transaction takes place. Hence we want to reduce the cost of $V=U^d \bmod p$ as much as possible. So we choose d a 160-bit number. A 160-bit discrete logarithm is safe against all current algorithms for computing discrete logarithm. The exponential computation with 160-bit exponent is much cheaper than that with a full-size exponent when the module has thousands of bits.

Computation Cost of Customer Both the computations $U=(D_j)^S$ mod p and V^R mod p are expensive. We can choose one of them cheaper by making the exponent small. We pick small R because it is possible to compute $U=(D_j)^S$ mod p and to download C_j in parallel in some cases.

Security Analysis

For a security analysis, we show that all the four requirements noted above are fulfilled. They are based on different computational assumptions such as computing discrete logarithms or factoring large integers etc.

1) No intention of the customer is disclosed

The privacy protection achieved is based on the assumption that there are many customers and that many digital goods are engaged in the transactions. If there is only one customer and only one good is downloaded, the privacy protection cannot be achieved. What is achieved is actually the unlinkability similar to the anonymous feature of digital cash. More precisely, if there are only two customers and the first customer buys A and the second customer buys B, there is no way for the merchant to tell who buys A and who buys B.

There are two cases. One is that A and B are from the same provider. The other is that A and B are from different providers.

For the first situation, the security is information-theoretically guaranteed, i.e., the merchant cannot tell who buys A and who buys B even if he has infinite computing power.

For the second situation, the security is based on the difficulty to factorize Q. So far the most efficient factoring algorithm is the so-called *number field sieve algorithm* that has complexity $L_Q(1/3, c)$, which is dependent on size of Q. But Q is large enough to resist the number field sieve algorithm. Elliptic curve factoring algorithm is dependent on the size of the smallest prime factor q of Q, but it has complexity $L_q(1/2, c)$, larger than

that of number field sieve algorithm. By elliptic curve factoring algorithm, the estimated computing cost to factor Q, whose smallest prime factor has 256 bit, is about 10^8 MIPS-years (million-instructions-per-second years). That is about 1/1000 of that of factoring a 1024-bit number of two prime factors by number field sieve algorithm. It is considered that 10^8 MIPS-years is an acceptable security level for privacy protection.

2) The customer can obtain only one digital object in one transaction

If the customer could obtain d from U and V in the step 9 of the scheme, the customer could obtain all the digital goods by buying only one of them. But that is equivalent to computing discrete logarithm. We specify d 160-bit just for dispelling that possibility. The second possibility for a dishonest customer is to find $D_{i,1}$, $D_{i,2}$, ..., $D_{i,k}$, $D_{i,k+1}$ such that $D_{i,1}D_{i,2}...D_{i,k}=D_{i,k+1} \bmod p$. In that case, the customer can obtain k+1 digital goods by paying k of them. But the probability to find such D's is negligible due to the size and randomness of r_1, r_2, ...,r_m. A similar attack is that the customer finds k+1 of D_i's such that they are all C-smooth and the number of the primes smaller than C is no larger than k. However, such a C must be too large to make the attack feasible due to the randomness of D_i's.

3) The auditing centre can conduct sale auditing

In step 8 of the scheme the customer blinds the ciphertext by $U=(D_j)^S \bmod p$. As long as S is co-prime with q_1, q_2, ... , q_t, U has the same order as that of D_j. Similarly, as long as s_j is co-prime with q_1, q_2, ... , q_t, the D_j has the same order as that of $g_{j'}$, where $M_j \in Provider_j'$. Since q_1, q_2, ... , q_t are kept secret by the auditing centre and the factorization of Q is infeasible, neither the merchant nor the customer can know any of q_1, q_2, ... , q_t. That means the probability that U has different order from that of $g_{j'}$ is negligibly small.

The above analysis is based on the assumption that the customer does not deliberately violate the protocol in order to undermine the sale auditing. He could do it by asking the merchant to conduct blinding decryption on D_i and ($D_i \cdot D_j \bmod p$). In that case he could obtain both D_i and D_j, but the auditing

centre would be misguided by the transcript of decrypting ($D_i \cdot D_j \bmod p$). The counter measure solution is to: Let the auditing centre select a random one-to-one function f: $\{0,1\}^t \rightarrow \{0,1\}^t$ and keep f secret. Let $p=2q_1q_2\ldots q_{t+2}+1$ instead of $p=2q_1q_2\ldots q_t+1$. Finally, let

$$g_i = g^{e_i} \bmod p$$

where $e_i = \prod_{j=1}^{t+2} (q_j)^{b_{ij}}$ and b_{ij} is the j-th bit of $f(i)$ in binary format for $j=1,2,\ldots,t$, while b_{it+1} and b_{it+2} are two checking bits of b_{ij}'s for $j=1,2,\ldots,t$ by hashing them. In this case, if a customer performs maliciously as above, he would be caught with probability 3/4. The cost of this solution is that the p has to have 512 more bits.

4) The auditing centre can never obtain any digital object

Although the auditing centre can recover the order of U, i.e., to "trace" U, there is no way for the auditing centre to "decrypt" U. The secret key K_j is beyond the auditing centre's reach forever.

Whilst the method and system of the present invention has been summarised and explained by illustrative application it will be appreciated by those skilled in the art that many widely varying embodiments and applications are within the teaching and scope of the present invention, and that the examples presented herein are by way of illustration only and should not be construed as limiting the scope of this invention.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method for trading digital goods online between a merchant and customer including the steps of:

said merchant encrypting each said digital good with respective unique keys to create encrypted goods;

said merchant encrypting each said respective unique key with a common key to create respective encrypted keys;

said merchant making each said encrypted good and each said respective encrypted key available to said customer;

said customer downloading one said encrypted good and respective encrypted key;

said customer adding a customer encryption to said respective encrypted key to create a combined key, and returning said combined key to said merchant;

said merchant removes common encryption from said combined key using said common key to create a customer encrypted key, and returns said customer encrypted key to said customer;

said customer decrypts said customer encrypted key to obtain said respective unique key and uses said respective unique key to decrypt said digital good.

2. A method as claimed in claim 1, wherein said merchant removes said common encryption following payment from said customer for said digital good.

3. A method as claimed in claim 1 or claim 2 wherein said digital goods may include one or more digital products.

4. A method for trading digital goods online between a merchant and customer including the steps of:

said merchant encrypting each said digital good with respective unique keys to create encrypted goods;

said merchant obtains parameters from an auditing centre;

said merchant encrypting each said respective unique key with a common key and using said parameters to create respective encrypted keys;

said merchant making each said encrypted good and each said respective encrypted key available to said customer;

said customer downloading one said encrypted good and respective encrypted key;

said customer adding a customer encryption to said respective encrypted key to create a combined key, and returning said combined key to said merchant;

said merchant removes common encryption from said combined key using said common key to create a customer encrypted key, and returns said customer encrypted key to said customer;

said customer decrypts said customer encrypted key to obtain said respective unique key and uses said respective unique key to decrypt said digital good.

5. A method as claimed in claim 4, further including the steps of:
said merchant collecting transcripts from removal of said common encryption and forwarding said transcripts to said auditing centre;

said auditing centre reviews said transcripts and obtains said parameters;

wherein said parameters are able to identify what goods were obtained by said customer.

6. A method as claimed in claim 4 or claim 5, wherein said merchant removes said common encryption following payment from said customer for said digital good.

7. A method as claimed in one of claims 4 to 6, wherein said digital goods may include one or more digital products.

8. A method as claimed in any one of claims 4 to 7, wherein said parameters are:

$$g_i = g^{e_i} \bmod p$$

where

$$e_i = \prod_{j=1}^{t} (q_j)^{b_{ij}}$$

and

$$p = 2\prod_{i=1}^{t} q_i + 1$$

and where

q are primes

$2^t >$ number of providers

b_{ij} is the j-th bit of i in binary format

9. A system for trading digital goods online between a merchant and customer wherein said goods are encrypted using parameters provided by an auditor, said customer obtaining said encrypted goods using blinding decryption such that said merchant is unable to identify said digital goods, said merchant providing transcripts of sale transfers to said auditor, said auditor using said transcripts and said parameters to identify goods and transferred.

10. A system as claimed in claim 9, wherein said merchant encrypts said digital goods.

11. A system as claimed in claim 9 or claim 10, wherein said customer obtains said encrypted goods following payment to said merchant.

12. A system as claimed in any one of claims 9 to 11, wherein said parameters are:

$$g_i = g^{e_i} \bmod p$$

where

$$e_i = \prod_{j=1}^{t} (q_j)^{b_{ij}}$$

and

$$p = 2\prod_{i=1}^{t} q_i + 1$$

and where

q are primes

$2^t >$ number of providers

b_{ij} is the j-th bit of i in binary format